48 P 17 64

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 14 084 C1** B2

(51) Int. Cl.[6]: **H 04 L 9/00**
G 06 F 12/14

(21) Aktenzeichen: 195 14 084.2-31
(22) Anmeldetag: 13. 4. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 11. 7. 96

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Horn, Günter, Dr., 81541 München, DE; Müller, Klaus, Dipl.-Math., 81539 München, DE; Kessler, Volker, Dr., 85256 Vierkirchen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 52 22 140
US 51 53 919
US-Z.: BELLER, M. et al.: Privacy and Authentication on a Portable Communications System. In: IEEE Journal on Selected Areas in Communications, Vol. 11,No. 6, August 1993, S. 821-829;
US-Z.: AZIZ, A., DIFFIE, W.: Privacy and Authentication for Wireless Local Area Networks. In: IEEE Personal Communications, 1994, S. 25-31;

(54) Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit U und einer Netzcomputereinheit N

(57) Die Erfindung betrifft ein Verfahren zum Austausch kryptographischer Schlüssel, bei dem die Länge der übertragenen Nachrichten wesentlich reduziert und die Sicherheitseigenschaften des Verfahrens gegenüber bekannten Verfahren erheblich erweitert werden.
In einer Netzcomputereinheit und in einer Benutzercomputereinheit werden ein erster Zwischenschlüssel und ein zweiter Zwischenschlüssel abhängig von generierten Zufallszahlen gebildet.
Ein Sitzungsschlüssel wird durch eine bitweise Exklusiv-Oder-Verknüpfung des ersten Zwischenschlüssels und des zweiten Zwischenschlüssels berechnet. Die Schlüssel werden niemals in Klartext übertragen. Durch Verwendung einer Funktion, die z. B. eine symmetrische Verschlüsselungsfunktion, eine Hash-Funktion oder eine Einwegfunktion sein kann, authentifizieren sich die Netzcomputereinheit und die Benutzercomputereinheit gegenseitig.

DE 195 14 084 C1

Beschreibung

Informationstechnische Systeme unterliegen verschiedenen Bedrohungen. So kann z. B. übertragene Information von einem unbefugten Dritten abgehört und verändert werden. Eine weitere Bedrohung bei der Kommunikation zweier Kommunikationspartner liegt in der Vorspiegelung einer falschen Identität eines Kommunikationspartners.

Diesen und weiteren Bedrohungen wird durch verschiedene Sicherheitsmechanismen, die das informationstechnische System vor den Bedrohungen schützen sollen, begegnet. Ein zur Sicherung verwendet er Sicherheitsmechanismus ist die Verschlüsselung der übertragenen Daten. Damit die Daten in einer Kommunikationsbeziehung zwischen zwei Kommunikationspartnern verschlüsselt werden können, müssen vor der Übertragung der eigentlichen Daten erst Schritte durchgeführt werden, die die Verschlüsselung vorbereiten. Die Schritte können z. B. darin bestehen, daß sich die beiden Kommunikationspartner auf einen Verschlüsselungsalgorithmus einigen und ggf. die gemeinsamen geheimen Schlüssel vereinbart werden.

Besondere Bedeutung gewinnt der Sicherheitsmechanismus Verschlüsselung bei Mobilfunksystemen, da die übertragenen Daten in diesen Systemen von jedem Dritten ohne besonderen zusätzlichen Aufwand abgehört werden können.

Dies führt zu der Anforderung, eine Auswahl bekannter Sicherheitsmechanismen so zu treffen und diese Sicherheitsmechanismen geeignet zu kombinieren, sowie Kommunikationsprotokolle zu spezifizieren, daß durch sie die Sicherheit von informationstechnischen Systemen gewährleistet wird.

Es sind verschiedene asymmetrische Verfahren zum rechnergestützen Austausch kryptographischer Schlüssel bekannt. Asymmetrische Verfahren, die geeignet sind für Mobilfunksysteme, sind (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) und (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11).

Das in (A. Aziz, W. Diffie: "Privacy and Authentication Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) beschriebene Verfahren bezieht sich ausdrücklich auf lokale Netzwerke und stellt höhere Rechenleistungsanforderungen an die Computereinheiten der Kommunikationspartner während des Schlüsselaustauschs. Außerdem wird in dem Verfahren mehr Übertragungskapazität benötigt als in dem erfindungsgemäßen Verfahren, da die Länge der Nachrichten größer ist als bei dem erfindungsgemäßen Verfahren.

Das in (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, Pages 1 bis 11) hat einige grundlegende Sicherheitsmechanismen nicht integriert. Die explizite Authentifikation des Netzes durch den Benutzer wird nicht erreicht. Außerdem wird ein vom Benutzer an das Netz übertragener Schlüssel vom Netz nicht an den Benutzer bestätigt. Auch eine Zusicherung der Frische (Aktualität) des Schlüssels für das Netz ist nicht vorgesehen. Ein weiterer Nachteil dieses Verfahrens besteht in der Beschränkung auf das Rabin-Verfahren bei der impliziten Authentifizierung des Schlüssels durch den Benutzer. Dies schränkt das Verfahren in einer flexibleren Anwendbarkeit ein. Außerdem ist kein Sicherheitsmechanismus vorgesehen, der die Nichtabstreitbarkeit von übertragenen Daten gewährleistet. Dies ist ein erheblicher Nachteil vor allem auch bei der Erstellung unanfechtbarer Gebührenabrechnungen für ein Mobilfunksystem. Auch die Beschränkung des Verfahrens auf den National Institute of Standards in Technology Signature Standard (NIST DSS) als verwendete Signaturfunktion schränkt das Verfahren in seiner allgemeinen Verwendbarkeit ein.

Das Problem der Erfindung liegt darin, ein Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel anzugeben, das die oben genannten Nachteile vermeidet.

Dieses Problem wird durch das Verfahren gemäß Patentanspruch 1 gelöst.

Die durch das erfindungsgemäße Verfahren erreichten Vorteile liegen vor allem in dem Bereich einer höheren Sicherheit des erfindungsgemäßen Verfahrens im Vergleich zu bekannten Verfahren und in einer erheblichen Reduktion der Länge der übertragenen Nachrichten. Durch das erfindungsgemäße Verfahren werden folgende Sicherheitsmechanismen realisiert:

- Gegenseitige explizite Authentifizierung von dem Benutzer und dem Netz, d. h. die gegenseitige Verifizierung der behaupteten Identität,
- Schlüsselvereinbarung zwischen dem Benutzer und dem Netz mit gegenseitiger impliziter Authentifizierung, d. h. daß durch das Verfahren erreicht wird, daß nach Abschluß der Prozedur ein gemeinsamer geheimer Sitzungsschlüssel zur Verfügung steht, von dem jede Partei weiß, daß nur das authentische Gegenüber sich ebenfalls im Besitz des geheimen Sitzungsschlüssels befinden kann,
- Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für den Benutzer und das Netz,
- gegenseitige Bestätigung des Sitzungsschlüssels von dem Benutzer und dem Netz, d. h. die Bestätigung, daß das Gegenüber tatsächlich im Besitz des vereinbarten geheimen Sitzungsschlüssels ist,
- Benutzeranonymität, d. h. Vertraulichkeit der Identität des Benutzers gegenüber Dritten,
- Nichtabstreitbarkeit von Daten, die vom Benutzer an das Netz gesendet wurden, durch den Benutzer.
- Senden eines Zertifikats für den öffentlichen Schlüssel des Netzes vom Netz an den Benutzer,
- Senden eines Zertifikats für den öffentlichen Schlüssel des Benutzers von der Zertifizierungsinstanz an das Netz.

Außerdem liegt ein erheblicher Vorteil des erfindungsgemäßen Verfahrens darin, daß ein im Vergleich zu einem symmetrischen Verschlüsselungsalgorithmus die sehr rechenintensive modulare Exponentiation nur zwei Mal auf jeder Seite durchgeführt werden muß, was eine wesentlich höhere Protokollabarbeitungsgeschwindigkeit ermöglicht.

Die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 3 realisiert zusätzlich einen weiteren Sicherheitsmechanismus, den Austausch von Zertifikaten für öffentliche Schlüssel zwischen dem Benutzer und dem Netz.

Das erfindungsgemäße Verfahren ist außerdem sehr leicht an unterschiedliche Anforderungen anpaßbar, da es sich nicht auf bestimmte Verschlüsselungsalgorith-

men beschränkt.

Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die Zeichnungen stellen bevorzugte Ausführungsbeispiele der Erfindung dar, die im folgenden näher beschrieben werden.

Es zeigen

Fig. 1a, b ein Ablaufdiagramm, das das erfindungsgemäße Verfahren gemäß Patentanspruch 1 darstellt;

Fig. 2a, b eine Skizze, die das erfindungsgemäße Verfahren gemäß Patentanspruch 3 darstellt.

Anhand der Fig. 1a, b und 2a, b wird die Erfindung weiter erläutert.

In den Fig. 1a, b ist durch eine Skizze der Ablauf des erfindungsgemäßen Verfahrens gemäß Patentanspruch 1 dargestellt. Bei diesem Verfahren wird vorausgesetzt, daß in einer Benutzercomputereinheit U ein vertrauenswürdiger öffentlicher Netzschlüssel g^s verfügbar ist. Außerdem wird vorausgesetzt, daß in einer Netzcomputereinheit N ein vertrauenswürdiger öffentlicher Benutzerschlüssel g^u verfügbar ist.

Das in den Fig. 1a, b beschriebene erfindungsgemäße Verfahren beginnt mit einer Generierung einer ersten Zufallszahl t in der Netzcomputereinheit N. Aus der ersten Zufallszahl t wird von einem erzeugenden Element g einer endlichen Gruppe in der Netzcomputereinheit N ein erster Wert g^t gebildet.

Asymmetrische Verfahren beruhen im wesentlichen auf zwei Problemen der Komplexitätstheorie, dem Problem zusammengesetzte Zahlen effizient zu faktorisieren, und dem diskreten Logarithmusproblem (DLP). Das DLP besteht darin, daß in geeigneten Rechenstrukturen zwar Exponentiationen effizient durchgeführt werden können, daß jedoch für die Umkehrung dieser Operation, das Logarithmieren, keine effizienten Algorithmen bekannt sind. Solche Rechenstrukturen sind unter den oben bezeichneten endlichen Gruppen zu verstehen. Diese sind z. B. die multiplikative Gruppe eines endlichen Körpers (z. B. Multiplizieren modulo p, wobei p eine große Primzahl ist), oder auch sogenannte "elliptische Kurven". Elliptische Kurven sind vor allem deshalb interessant, weil sie bei gleichem Sicherheitsniveau wesentlich kürzere Sicherheitsparameter erlauben. Dies betrifft die Länge der öffentlichen Schlüssel, die Länge der Zertifikate, die Länge der bei der Sitzungsschlüsselvereinbarung auszutauschenden Nachrichten sowie die Länge von digitalen Signaturen, die jeweils im weiteren beschrieben werden. Der Grund dafür ist, daß die für elliptische Kurven bekannten Logarithmierverfahren wesentlich weniger effizient sind als die für endliche Körper. Eine große Primzahl in diesem Zusammenhang bedeutet, daß die Größe der Primzahl so gewählt werden muß, daß die Logarithmierung so aufwendig ist, daß sie nicht in vertretbarer Zeit durchgeführt werden kann. Vertretbar bedeutet in diesem Zusammenhang einen Zeitraum entsprechend der Sicherheitspolitik für das informationstechnische System von mehreren Jahren bis Jahrzehnten und länger.

Nach der Berechnung des ersten Wertes g^t wird eine erste Nachricht M1 gebildet, die mindestens den ersten Wert g^t aufweist. Die erste Nachricht M1 wird in der Netzcomputereinheit N codiert und an die Benutzercomputereinheit U übertragen. In der Benutzercomputereinheit U wird die erste Nachricht M1 decodiert.

Außerdem wird in der Benutzercomputereinheit U eine zweite Zufallszahl r gebildet. Aus der zweiten Zufallszahl r wird ein zweiter Wert g^r von dem erzeugenden Element g entsprechend der gewählten im vorigen beschriebenen Rechenstruktur berechnet.

Ein öffentlicher Netzschlüssel, der in der Benutzercomputereinheit verfügbar ist, wird potenziert mit der zweiten Zufallszahl r und bildet somit einen ersten Zwischenschlüssel K1.

Mit dem ersten Zwischenschlüssel K1 wird unter Verwendung eines Verschlüsselungsalgorithmus Enc eine Identitätsangabe IMUI der Benutzercomputereinheit U verschlüsselt. Die verschlüsselte Identitätsangabe IMUI bildet einen ersten verschlüsselten Term VT1.

Außerdem wird in der Benutzercomputereinheit U ein zweiter Zwischenschlüssel K2 berechnet, indem der erste Wert g^t mit einem geheimen Benutzerschlüssel u potenziert wird.

Ein Sitzungsschlüssel K wird berechnet durch die bitweise Anwendung der Funktion Exklusiv-Oder auf den ersten Zwischenschlüssel K1 und den zweiten Zwischenschlüssel K2. Eine erste Antwort A wird gebildet durch Verschlüsselung einer Benutzerkonstanten constu, die sowohl der Benutzercomputereinheit U als auch der Netzcomputereinheit N bekannt ist, mit dem Sitzungsschlüssel K unter Verwendung einer Funktion f.

Die Funktion f kann z. B. eine symmetrische Verschlüsselungsfunktion sein oder eine Hash-Funktion oder eine Einwegfunktion. Unter einer Einwegfunktion ist in diesem Zusammenhang eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Unter einer Hash-Funktion ist eine komprimierende Einwegfunktion zu verstehen, wobei bei einer Hash-Funktion eine beliebig lange Eingangszeichenfolge auf eine Ausgangszeichenfolge fester Länge abgebildet wird. Des weiteren wird für die Einwegfunktion bzw. Hash-Funktion in diesem Zusammenhang Kollisionsfreiheit gefordert, d. h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben. Bekannte Hash-Funktionen sind z. B. der MD2-Algorithmus oder der MD5-Algorithmus.

In der Benutzercomputereinheit U wird anschließend eine zweite Nachricht M2 gebildet, wobei die zweite Nachricht M2 mindestens den zweiten Wert g^r, den ersten verschlüsselten Term VT1 und die erste Antwort A enthält. Die zweite Nachricht M2 wird in der Benutzercomputereinheit U codiert und an die Netzcomputereinheit N übertragen.

Durch den in der zweiten Nachricht M2 übertragenen zweiten Wert g^r ist es der Netzcomputereinheit N möglich, den ersten Zwischenschlüssel K1 selbst zu bilden, ohne daß der erste Zwischenschlüssel K1 übertragen werden muß. Dies wird erreicht, da nur die Benutzercomputereinheit U und die Netzcomputereinheit N im Besitz des ersten Zwischenschlüssels K1 sind.

Die erste Antwort A dient zur Verifizierung des Sitzungsschlüssels, den die Netzcomputereinheit N wie im weiteren beschrieben auch bilden kann, ohne daß der Sitzungsschlüssel K übertragen werden müßte.

Nach Empfang der zweiten Nachricht M2 wird die zweite Nachricht M2 in der Netzcomputereinheit N decodiert. Anschließend wird der erste Zwischenschlüssel K1 in der Netzcomputereinheit N berechnet, indem der zweite Wert g^r potenziert wird mit einem geheimen Netzschlüssel s. Damit ist es der Netzcomputereinheit N möglich, den übertragenen ersten verschlüsselten Term VT1 zu entschlüsseln mit dem in vorigen berechneten ersten Zwischenschlüssel K1.

Die Entschlüsselung des ersten verschlüsselten Terms VT1 wird durchgeführt und damit wird die Benutzer-

computereinheit U authentifiziert als Sender der zweiten Nachricht M2. Aus der Potenzierung eines öffentlichen Benutzerschlüssels g^u, der in vertrauenswürdiger Weise in der Netzcomputereinheit N verfügbar ist, mit der ersten Zufallszahl t wird der zweite Zwischenschlüssel K2 in der Netzcomputereinheit N gebildet.

Der Sitzungsschlüssel K wird in der Netzcomputereinheit N ebenso, wie in der Benutzercomputereinheit U, durch bitweise Exklusiv-Oder-Verknüpfung des ersten Zwischenschlüssels K1 mit dem zweiten Zwischenschlüssel K2 berechnet.

Mit Hilfe des Sitzungsschlüssels K wird unter Verwendung der Funktion f die erste Antwort A überprüft. Die Überprüfung kann, je nachdem welcher Art die Funktion f ist, auf unterschiedliche Weise geschehen.

Die explizite Authentifikation der Benutzercomputereinheit (U) wird durch die erste Antwort (A) erreicht, da, außer der Netzcomputereinheit (N) nur die Benutzercomputereinheit (U) den Sitzungsschlüssel (K) kennt.

Wenn die Funktion f durch eine symmetrische Verschlüsselungsfunktion realisiert wird, ist es möglich, die Überprüfung der ersten Antwort A auf zwei Arten durchzuführen:

Die der Netzcomputereinheit N bekannte Benutzerkonstante constu kann mit dem Sitzungsschlüssel K unter Verwendung der Funktion f in der Netzcomputereinheit N verschlüsselt werden und das Ergebnis kann mit der ersten Antwort A direkt verglichen werden. Bei Übereinstimmung des Ergebnisses mit der ersten Antwort A ist die Korrektheit des Schlüssels K gewährleistet.

Es ist jedoch auch möglich, die erste Antwort A mit dem in der Netzcomputereinheit N berechneten Sitzungsschlüssel K zu entschlüsseln, und eine dadurch erhaltene entschlüsselte Benutzerkonstante constu' mit der bekannten Benutzerkonstante constu zu vergleichen. Bei Übereinstimmung der Benutzerkonstante constu mit der entschlüsselten Benutzerkonstante constu' ist ebenso die Korrektheit des Sitzungsschlüssels K garantiert.

Wird die Funktion f durch eine Hash-Funktion realisiert, so ist die Entschlüsselung der ersten Antwort A naturgemäß nicht möglich. Somit ist es in diesem Fall nur möglich, die Überprüfung so zu gestalten, daß die Benutzerkonstante constu und der Sitzungsschlüssel K unter Anwendung der Funktion f ein Ergebnis liefert, das mit der ersten Antwort A verglichen wird.

Anschließend wird in der Netzcomputereinheit N eine Netzkonstante constn mit dem überprüften Sitzungsschlüssel K unter Verwendung der Funktion f verschlüsselt und bildet eine zweite Antwort B.

In der Netzcomputereinheit N wird eine dritte Nachricht M3 gebildet, die mindestens die zweite Antwort B enthält. Die dritte Nachricht M3 wird in der Netzcomputereinheit N codiert und an die Benutzercomputereinheit U übertragen.

In der Benutzercomputereinheit U wird die dritte Nachricht M3 decodiert und im Anschluß daran die zweite Antwort in entsprechender Weise überprüft, wie dies im vorigen für die erste Antwort A in der Netzcomputereinheit N beschrieben wurde.

Für den Fall, daß in der Benutzercomputereinheit U der öffentliche Netzschlüssel g^s und in der Netzcomputereinheit N der öffentliche Benutzerschlüssel g^u nicht bekannt sind bzw. nicht in vertrauenswürdiger Weise vorliegen, wird eine Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 3 verwendet. Diese Weiterbildung der Erfindung ist in den Fig. 2a, b dargestellt.

Wenn zum Austausch des öffentlichen Netzschlüssels g^s und des öffentlichen Benutzerschlüssels g^u die Verwendung eines Benutzerzertifikats CertU und eines Netzzertifikats CertN vorgesehen sind, so kann es vorteilhaft sein, wenn bei Vorhandensein mehrerer vertrauenswürdiger Zertifizierungsinstanzen die Benutzercomputereinheit U der Netzcomputereinheit N mitteilt, von welcher Zertifizierungsinstanz die Benutzercomputereinheit U ein Netzzertifikat CertN verifizieren kann.

Dies kann z. B. dadurch geschehen, daß zu Beginn des erfindungsgemäßen Verfahrens eine Zertifizierungsnachricht von der Benutzercomputereinheit U an die Netzcomputereinheit N übertragen wird. Die Zertifizierungsnachricht weist in diesem Zusammenhang mindestens eine Identitätsangabe einer Zertifizierungscomputereinheit auf, von der die Netzcomputereinheit N ein Netzzertifikat CertN erhalten kann, das von der Benutzercomputereinheit U verifiziert werden kann.

Nachdem die Netzcomputereinheit N das Netzzertifikat CertN von der Zertifizierungscomputereinheit CA beschafft hat, wird das Netzzertifikat CertN an die Benutzercomputereinheit U übertragen.

Dies geschieht dadurch, daß der ersten Nachricht M1 zusätzlich das Netzzertifikat CertN beigefügt wird. In der Benutzercomputereinheit U wird nach der Decodierung der ersten Nachricht M1 in diesem Fall das Netzzertifikat CertN verifiziert und somit hat die Benutzercomputereinheit U einen vertrauenswürdigen öffentlichen Netzschlüssel g^s erhalten.

In der Benutzercomputereinheit U wiederum wird ein Benutzerzertifikat CertU ermittelt, und anstelle der Identitätsangabe IMUI der Benutzercomputereinheit U mit dem ersten Zwischenschlüssel K1 unter Verwendung der Verschlüsselungsfunktion Enc zu dem ersten verschlüsselten Term VT1 verschlüsselt. Somit wird die Übertragung des Benutzerzertifikats CertU ermöglicht, ohne daß die Identität der Benutzercomputereinheit U an einen unbefugten Dritten bei der Übertragung der zweiten Nachricht M2 offenbart wird. Nach Entschlüsselung des ersten Terms VT1 in der Netzcomputereinheit N wird das dadurch erhaltene Benutzerzertifikat Certu von der Netzcomputereinheit N verifiziert. Auf diese Weise ist ein vertrauenswürdiger Austausch von Netzzertifikat CertN und dem Benutzerzertifikat CertU erreicht.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit (U) und einer Netzcomputereinheit (N),

— bei dem in der Netzcomputereinheit (N) eine erste Zufallszahl (t) generiert wird,

— bei dem in der Netzcomputereinheit (N) aus der ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe ein erster Wert (g^t) berechnet wird,

— bei dem in der Netzcomputereinheit (N) eine erste Nachricht (M1) gebildet wird, die mindestens den ersten Wert (g^t) aufweist,

— bei dem die erste Nachricht (M1) von der Netzcomputereinheit (N) an die Benutzercomputereinheit (U) übertragen wird,

— bei dem in der Benutzercomputereinheit (U) eine zweite Zufallszahl (r) generiert wird,

— bei dem in der Benutzercomputereinheit

(U) aus der zweiten Zufallszahl (r) ein zweiter Wert (g^r) mit Hilfe des erzeugenden Elements (g) einer endlichen Gruppe gebildet wird,

— bei dem in der Benutzercomputereinheit (U) ein erster Zwischenschlüssel (K1) berechnet wird in der Weise, daß ein öffentlicher Netzschlüssel (g^s) potenziert wird mit der zweiten Zufallszahl (r),

— bei dem in der Benutzercomputereinheit (U) ein erster verschlüsselter Term (VT1) berechnet wird durch Verschlüsselung einer Identitätsangabe (IMUI) der Benutzercomputereinheit (U) mit dem ersten Zwischenschlüssel (K1) unter Verwendung einer Verschlüsselungsfunktion (Enc),

— bei dem in der Benutzercomputereinheit (U) ein zweiter Zwischenschlüssel (K2) berechnet wird in der Weise, daß der erste Wert (g^t) potenziert wird mit einem geheimen Benutzerschlüssel (u),

— bei dem in der Benutzercomputereinheit (U) ein Sitzungsschlüssel (K) berechnet wird durch bitweise Exklusiv-Oder-Verknüpfung des ersten Zwischenschlüssels (K1) mit dem zweiten Zwischenschlüssel (K2),

— bei dem in der Benutzercomputereinheit (U) eine erste Antwort (A) gebildet wird durch Anwendung einer Funktion (f) auf eine Benutzerkonstante (constu) und den Sitzungsschlüssel (K) gebildet wird,

— bei dem in der Benutzercomputereinheit (U) eine zweite Nachricht (M2) gebildet wird, die mindestens den zweiten Wert (g^r), den ersten verschlüsselten Term (VT1) und die erste Antwort (A) aufweist,

— bei dem die zweite Nachricht (M2) von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird,

— bei dem in der Netzcomputereinheit (N) der erste Zwischenschlüssel (K1) berechnet wird in der Weise, daß der zweite Wert (g^r) potenziert wird mit einem geheimem Netzschlüssel (s),

— bei dem in der Netzcomputereinheit (N) der erste verschlüsselte Term (VT1) entschlüsselt wird,

— bei dem in der Netzcomputereinheit (N) die Identitätsangabe (IMUI) der Benutzercomputereinheit (U) überprüft wird,

— bei dem in der Netzcomputereinheit (N) der zweite Zwischenschlüssel (K2) berechnet wird, indem ein öffentlicher Benutzerschlüssel (g^u) potenziert wird mit der ersten Zufallszahl (t),

— bei dem in der Netzcomputereinheit (N) der Sitzungsschlüssel (K) berechnet wird durch bitweise Exklusiv-Oder-Verknüpfung des ersten Zwischenschlüssels (K1) mit dem zweiten Zwischenschlüssel (K2),

— bei dem in der Netzcomputereinheit (N) die erste Antwort (A) überprüft wird,

— bei dem in der Netzcomputereinheit (N) eine zweite Antwort (B) berechnet wird durch Anwendung der Funktion (f) auf eine Netzkonstante (constn) und den Sitzungsschlüssel (K) gebildet wird,

— bei dem eine dritte Nachricht (M3) von der Netzcomputereinheit (N) zu der Benutzercomputereinheit (U) übertragen wird, wobei die dritte Nachricht (M3) mindestens die zweite Antwort (B) enthält, und

— bei dem in der Benutzercomputereinheit (U) die zweite Antwort (B) überprüft wird.

2. Verfahren nach Anspruch 1, bei dem zu Beginn des Verfahrens eine Zertifizierungsnachricht von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird, wobei die Zertifizierungsnachricht mindestens eine Identitätsangabe einer Zertifizierungscomputereinheit enthält, die ein Netzzertifikat (CertN) liefert, das von der Benutzercomputereinheit (U) verifiziert werden kann.

3. Verfahren nach Anspruch 1 oder 2,

— bei dem die erste Nachricht (M1) zusätzlich ein Netzzertifikat (CertN) des öffentlichen Netzschlüssels (g^s) der Netzcomputereinheit (N) aufweist,

— bei dem in der Benutzercomputereinheit (U) das Netzzertifikat (CertN) verifiziert wird,

— bei dem in der Benutzercomputereinheit (U) der erste verschlüsselte Term (VT1) gebildet wird durch Verschlüsselung eines Benutzerzertifikats (CertU) eines öffentlichen Benutzerschlüssels (g^u) der Benutzercomputereinheit (U) mit dem ersten Zwischenschlüssel (K1) unter Verwendung einer Verschlüsselungsfunktion (Enc), und

— bei dem in der Netzcomputereinheit (N) das Benutzerzertifikat (CertU) verifiziert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,

— bei dem die Funktion (f) einen symmetrischen Verschlüsselungsalgorithmus, einen Hash-Algorithmus oder eine Einwegfunktion darstellt,

— bei dem die Überprüfung der ersten Antwort (A) in der Netzcomputereinheit (N) darin besteht, daß die Funktion (f) auf die Benutzerkonstante (constu) und den in der Netzcomputereinheit (N) berechneten Sitzungsschlüssel (K) angewendet wird und das Ergebnis mit der ersten Antwort (A) auf Übereinstimmung geprüft wird, und

— bei dem die Überprüfung der zweiten Antwort (B) in der Benutzercomputereinheit (U) darin besteht, daß die Funktion (f) auf die Netzkonstante (constn) und den in der Benutzercomputereinheit (U) berechneten Sitzungsschlüssel (K) angewendet wird und das Ergebnis mit der zweiten Antwort (B) auf Übereinstimmung geprüft wird.

5. Verfahren nach einem der Ansprüche 1 bis 3,

— bei dem die Funktion (f) einen symmetrischen Verschlüsselungsalgorithmus darstellt,

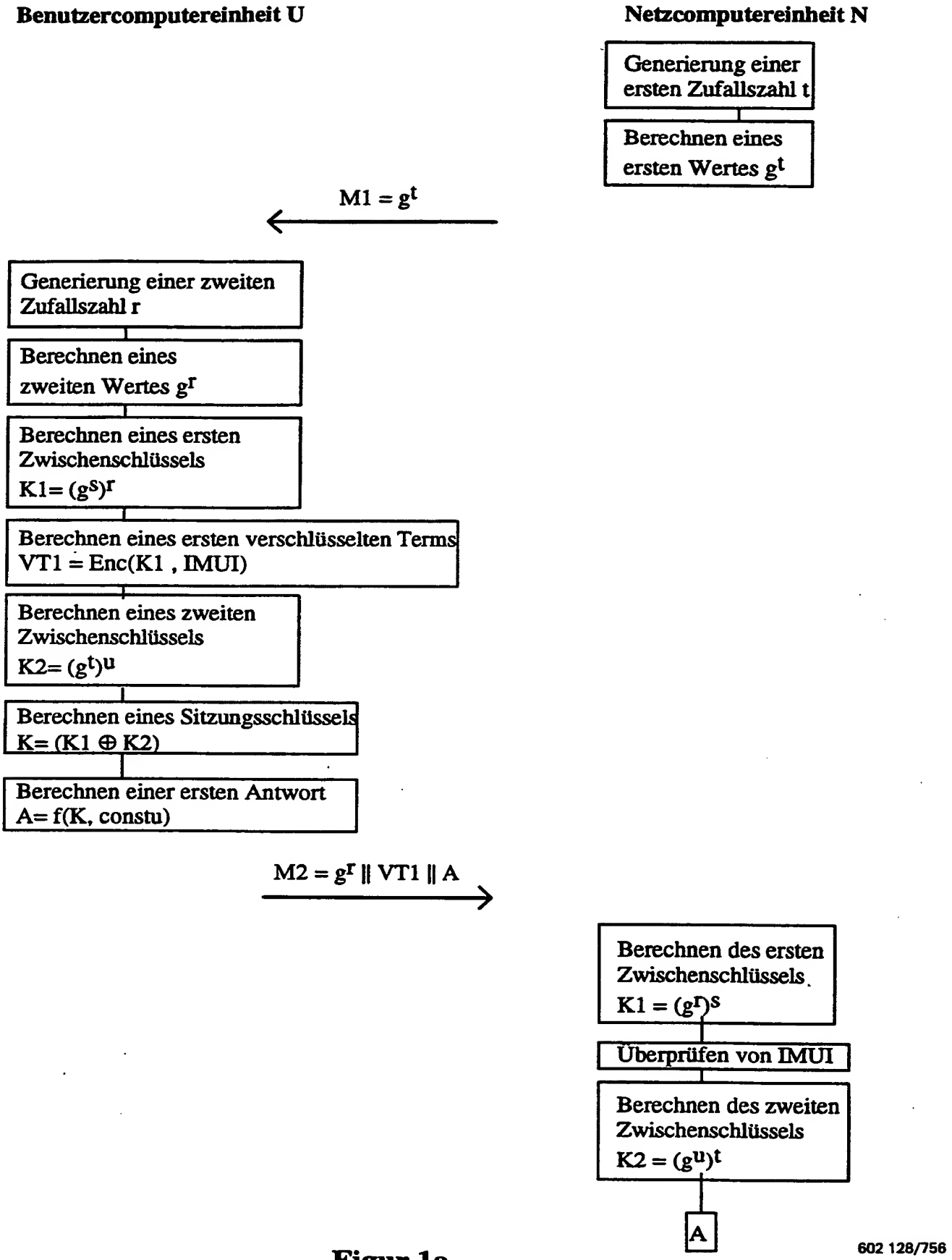
— bei dem die Überprüfung der ersten Antwort (A) in der Netzcomputereinheit (N) darin besteht, daß die erste Antwort (A) in der Netzcomputereinheit (N) mit dem in der Netzcomputereinheit (N) berechneten Sitzungsschlüssel (K) entschlüsselt wird und eine entschlüsselte Benutzerkonstante (constu) mit der Benutzerkonstante (constu) verglichen wird, und

— bei dem die Überprüfung der zweiten Antwort (B) in der Benutzercomputereinheit (U) darin besteht, daß die zweite Antwort (B) in der Benutzercomputereinheit (U) mit dem in der Benutzercomputereinheit (U) berechneten

Sitzungsschlüssel (K) entschlüsselt wird und eine entschlüsselte Netzkonstante (constn') mit der Netzkonstante (constn) verglichen wird.

Hierzu 4 Seite(n) Zeichnungen

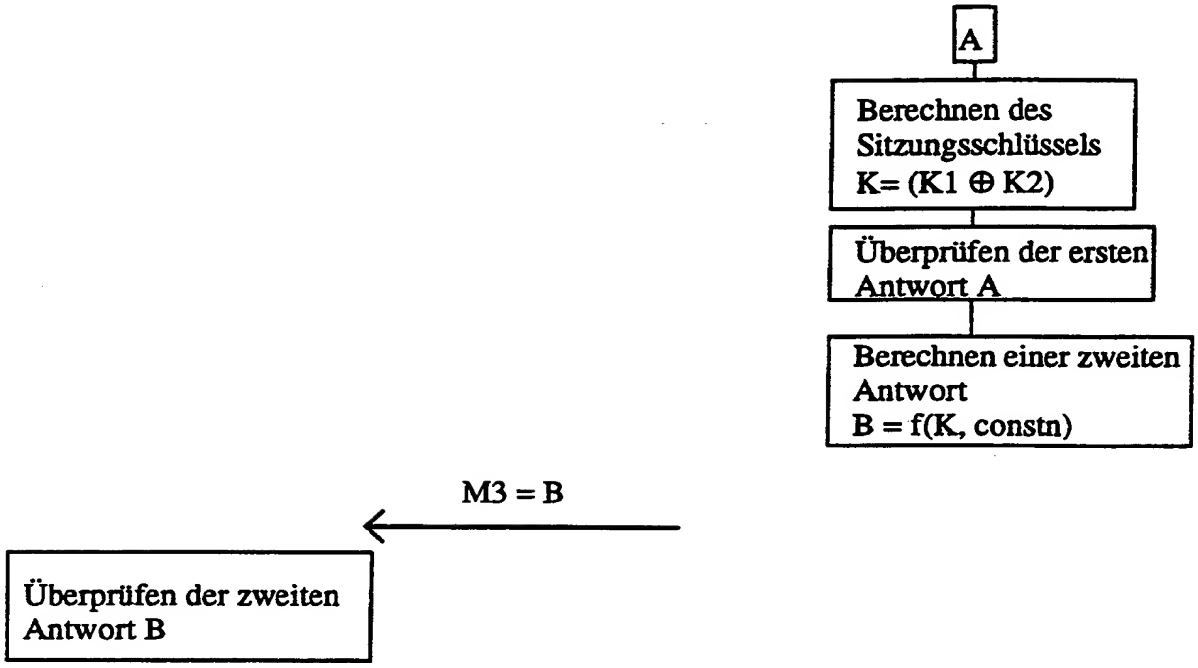
Nummer: DE 195 14 084 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 11. Juli 1996



Figur 1a

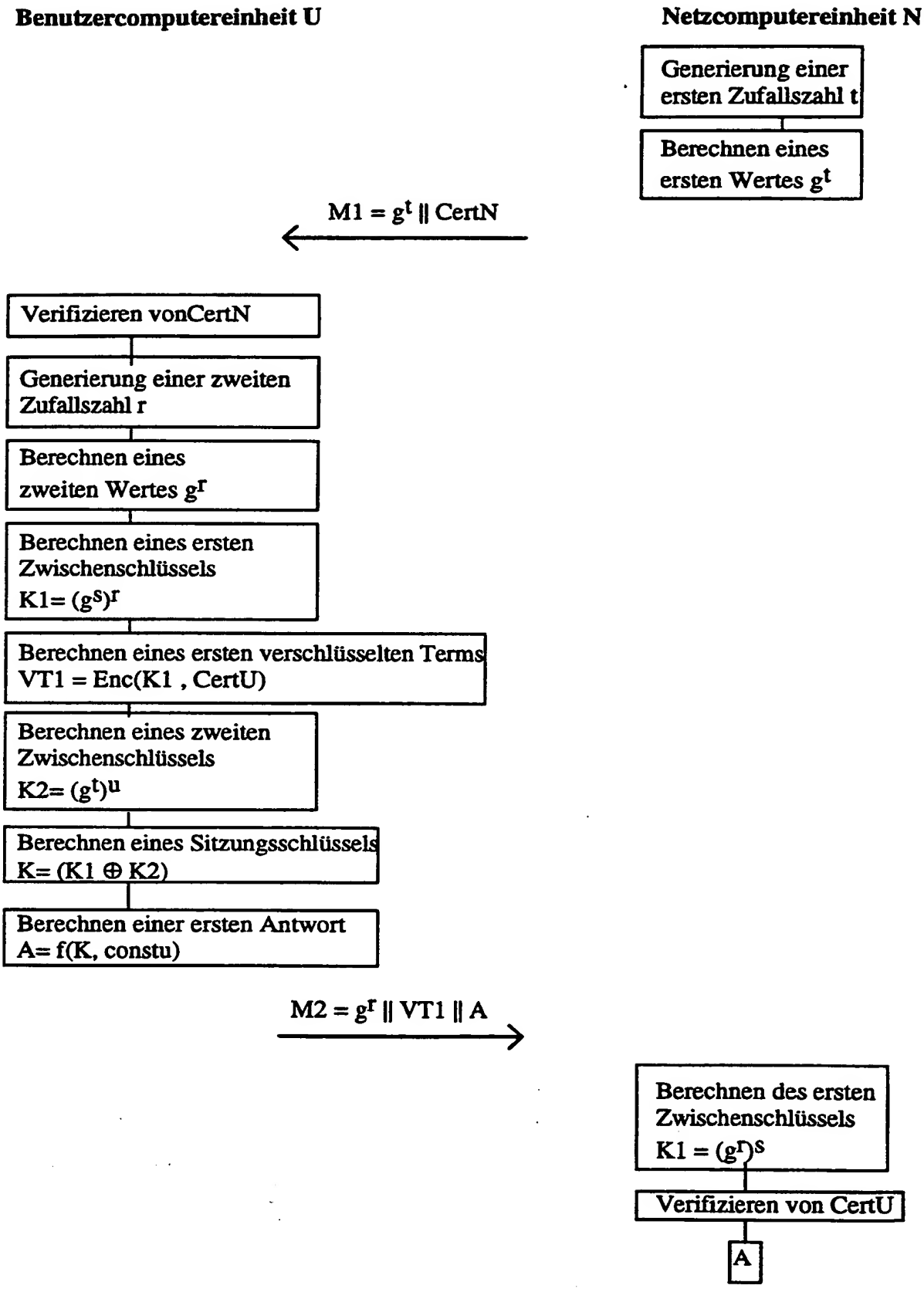
602 128/756

Nummer: DE 195 14 064 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 11. Juli 1996



Figur 1b

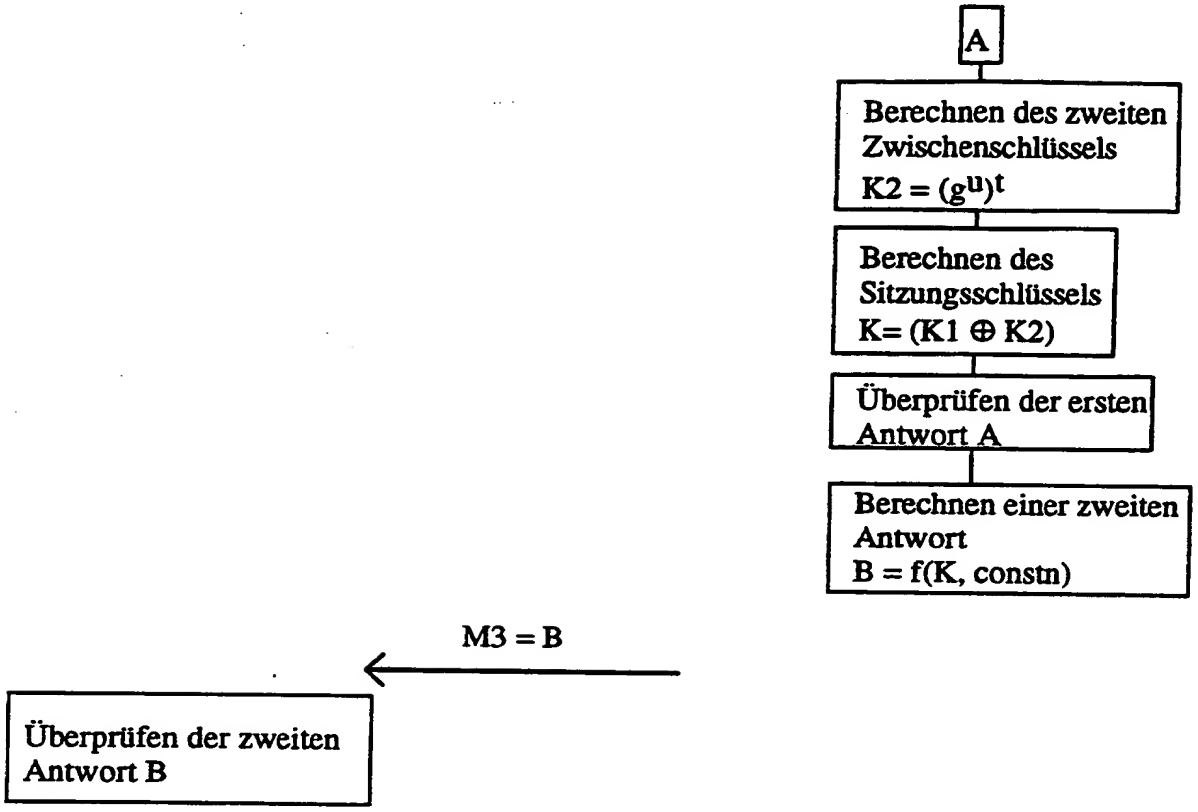
Nummer: DE 195 14 084 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 11. Juli 1996



Figur 2a

602 128/756

Nummer: DE 195 14 084 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 11. Juli 1996



Figur 2b

DOCKET NO: GR 98P 1764P
SERIAL NO: 09/700,928
APPLICANT: Horn et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100